Sophos Enterprise Console 5.3.0

Guia:

Manual de instalação do Sophos Enterprise Console 5.3.0

Versão 1

Data do Documento: Maio de 2015

Conteúdo

1. Sobre este manual

Este manual descreve os procedimentos necessários para realizar a instalação do Sophos Enterprise Console 5.3.0.

Com o Sophos Enterprise Console, é possível gerenciar todos os computadores protegidos pelo Sophos Endpoint, possibilitando inclusive o gerenciamento de diferentes sistemas operacionais e versões usando apenas uma interface.

2. Requisitos de Instalação

2.1. Requisitos para instalar o Sophos Enterprise Console:
http://www.sophos.com/en-us/support/knowledgebase/118635.aspx

2.2. Requisitos para instalar o Sophos Antivírus nos computadores da rede:

2.2.1. Windows: http://www.sophos.com/en-us/support/knowledgebase/118621.aspx

2.2.2. Linux: http://www.sophos.com/en-us/support/knowledgebase/118624.aspx

2.2.3. Mac OS X: http://www.sophos.com/en-us/support/knowledgebase/118623.aspx

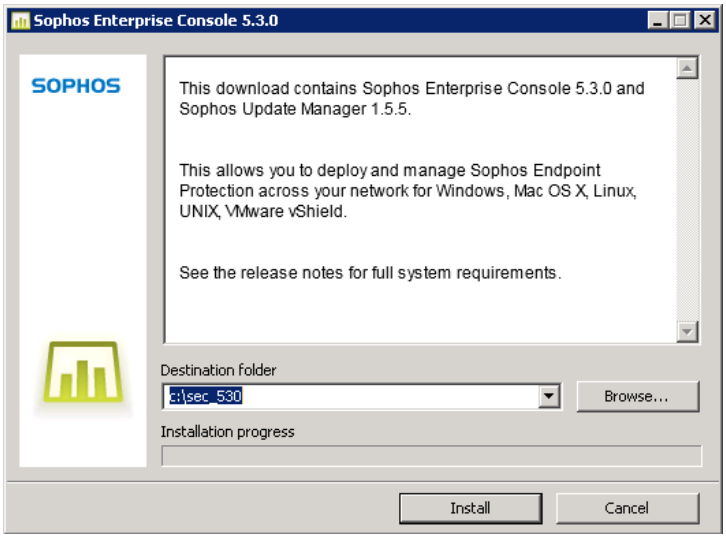
2.2.4. NetApp: http://www.sophos.com/en-us/support/knowledgebase/118633.aspx

2.2.5. UNIX: http://www.sophos.com/en-us/support/knowledgebase/118625.aspx

3. Instalando o Sophos Enterprise Console

3.1. Faça download e execute o arquivo “sec_530_sfx.exe”, link para download: http://downloads.m3corp.com.br/sophos10/sec_530_sfx.exe

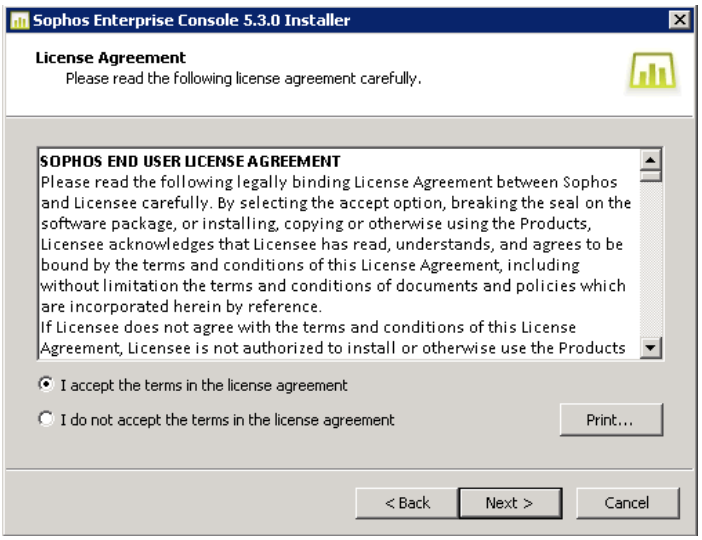
3.2. Clique no botão “Install”.



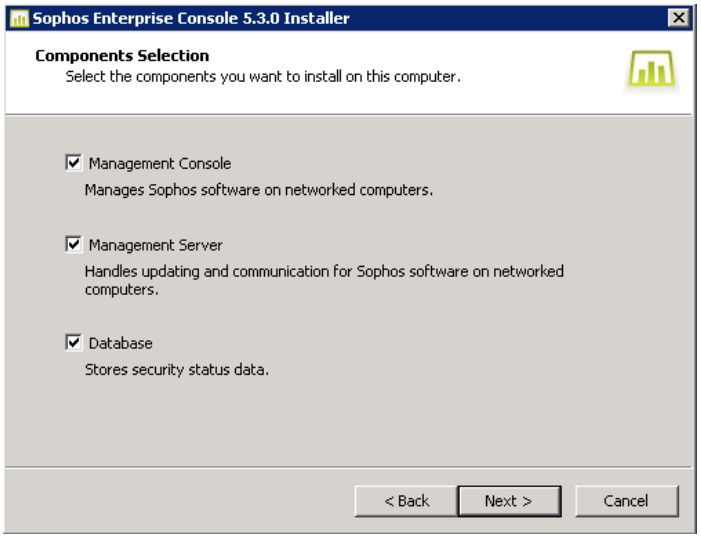
3.3. Aguarde enquanto os arquivos de instalação são extraídos.

3.4. Clique no botão “Avançar”.

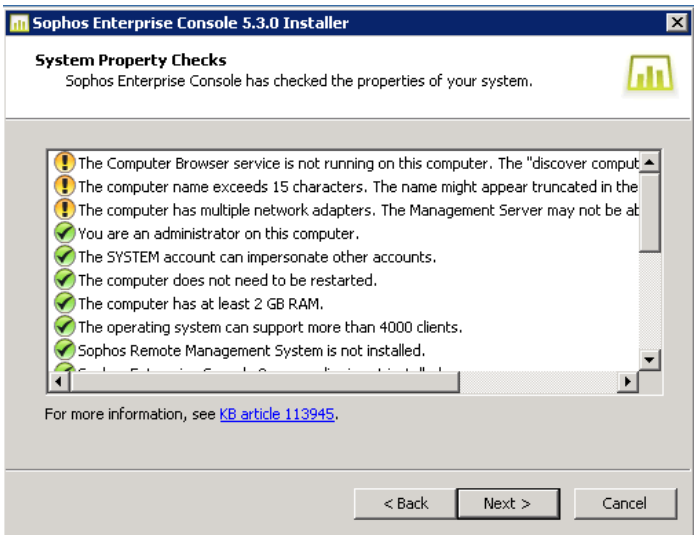
3.5. Clique em “I accept the terms in the license agreement” e clique no botão “Avançar”.



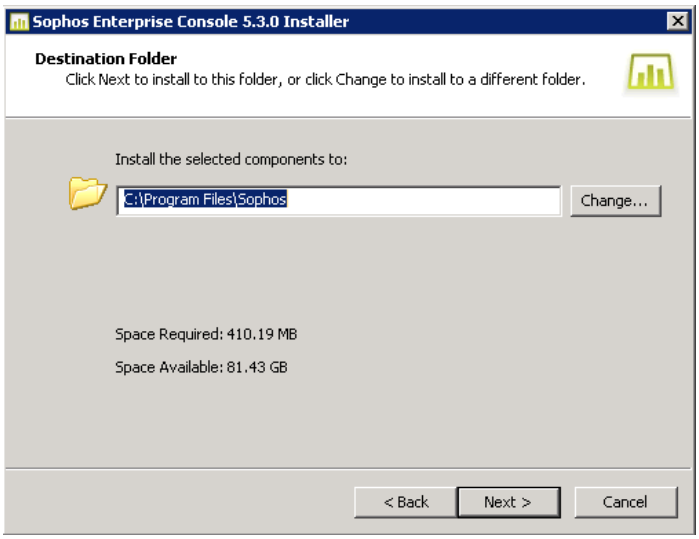
3.6. Verifique se as três opções estão selecionadas e clique em “Avançar”.



3.7. Caso algum item crítico for detectado, o item será sinalizado com o símbolo , itens críticos devem ser corrigidos antes de prosseguir com a instalação. Em caso de dúvida sobre algum item listado, verifique o artigo 113945 da Sophos (http://www.sophos.com/support/knowledgebase/article/113945.html)



3.8. Na tela “Destination Folder”, clique no botão “Avançar”.



3.9. Na tela “Database Details”, selecione a opção “Create a new instance called ‘SOPHOS’”.

3.10. Clique no botão “Browse”.

3.11. Caso o computador esteja em um domínio no entanto o computador **não** é o “domain controller” (servidor do Active Directory):

3.11.1. Clique no botão “Locais”.

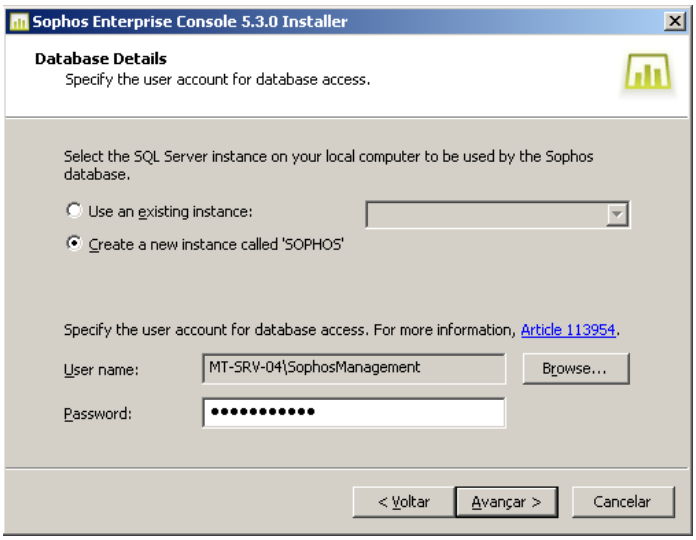
3.11.2. Selecione o nome do computador onde a instalação está sendo executado.

3.11.3. Clique no botão “OK”.

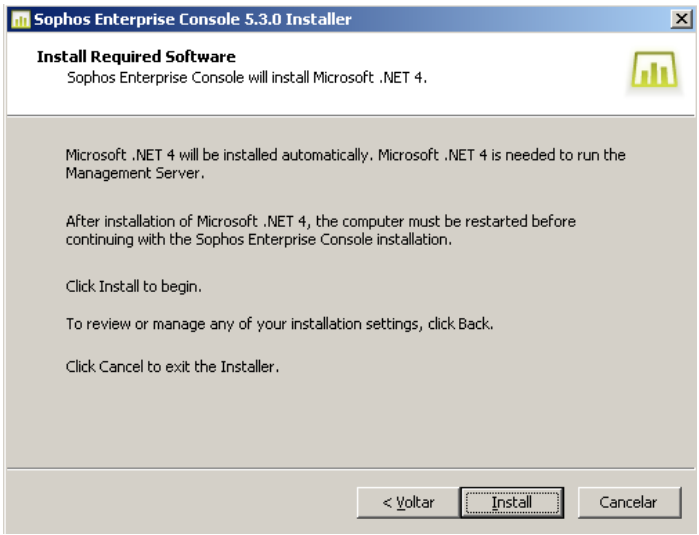
3.12. Informe o usuário “SophosManagement” e clique no botão “OK”.

3.13. Em “Password”, informe: **!s0ph0sMGR!**

3.14. Clique no botão “Avançar”.

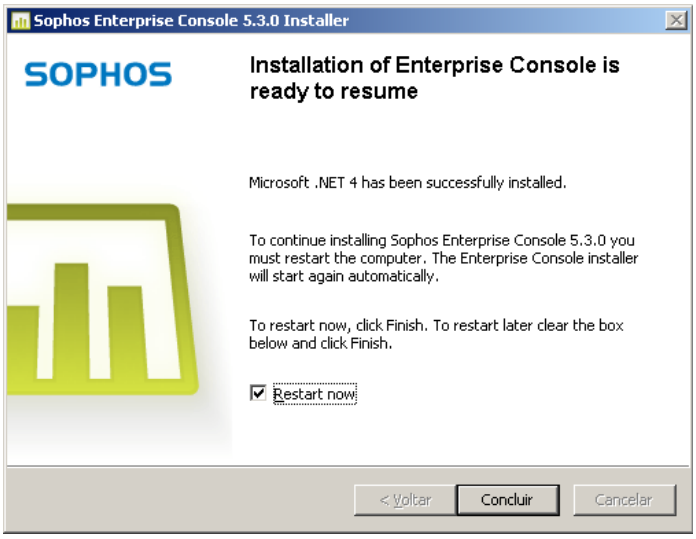


3.15. Caso o “.NET Framework 4” não esteja instalado, o wizard de instalação irá realizar a instalação do mesmo. Neste caso clique no botão “Install”.



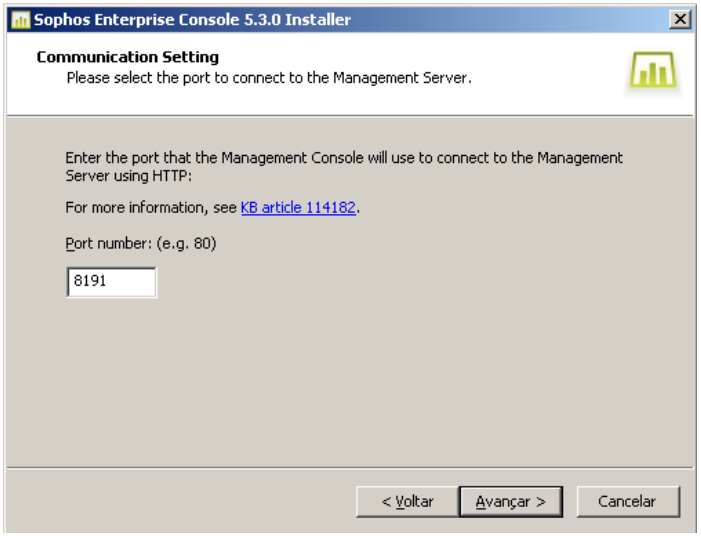
3.16. Caso o ".NET Framework 4" tenha sido instalado, será solicitada a reinicialização do computador, clique em "Concluir" para reinicia-lo. Caso não queira reiniciar o computador neste momento, desmarque a opção "Restart now" e clique em "Concluir". Após reiniciar, volte para o passo 3.4.

OBS: Após reiniciar o computador, o instalador será executado automaticamente, caso o mesmo usuário seja usado no logon. Caso seja necessário executar o instalador manualmente, execute o arquivo "C:\sec_530\ServerInstaller\Setup.exe".



3.17. O mesmo que ocorreu com o ".NET Framework 4" ocorrerá também com o requisito "Windows Installer 4.5", caso o mesmo não esteja instalado.

3.18. Na tela "Communication Setting", altere a porta para "8191" e clique no botão "Avançar".



3.19. Na tela "Sophos Update Manager Credentials", clique no botão "Browse".

3.20. Caso o computador esteja em um domínio, no entanto o computador não é o "domain controller" (servidor do Active Directory):

3.20.1. Clique no botão “Locais”.

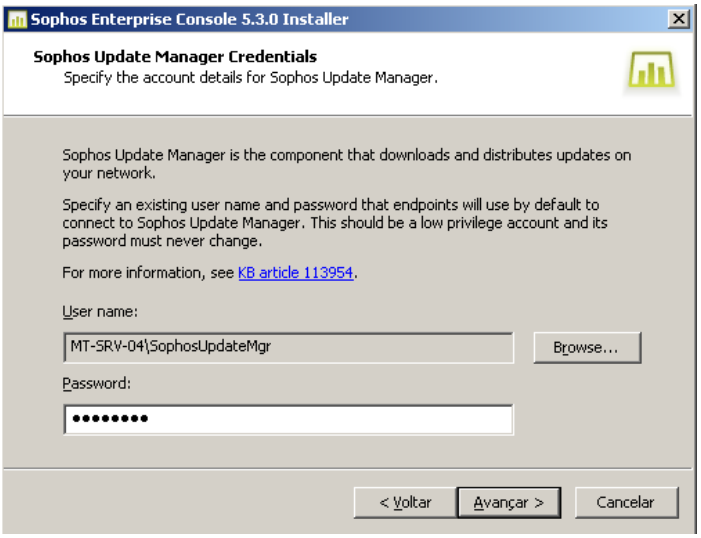
3.20.2. Selecione o nome do computador onde a instalação está sendo executado.

3.20.3. Clique no botão “OK”.

3.21. Informe o usuário “SophosUpdateMgr” e clique no botão “OK”.

3.22. Em “Password”, informe: **!s0ph0s!**

3.23. Clique em “Avançar”.



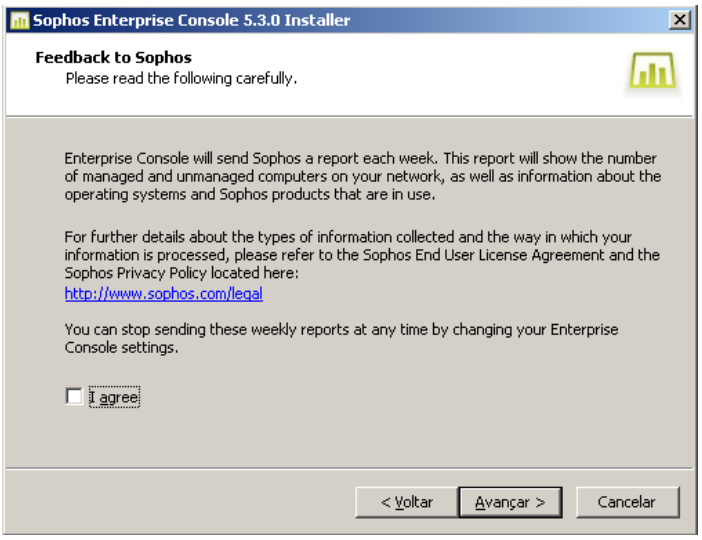
3.24. Na tela “Manage Encryption”, marque a opção “Do not manage encryption” e clique em “Avançar.

IMPORTANTE:

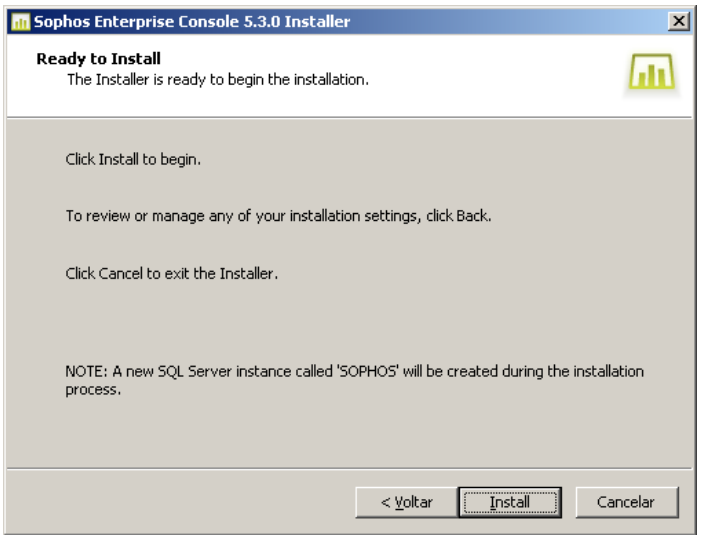
A funcionalidade de Full Disk Encryption (SDE) já não está mais disponível para novas aquisições de produto.

O suporte a essa funcionalidade permanece até Março de 2016, porém somente para os clientes que já haviam adquirido o produto com essa funcionalidade antes da descontinuação.

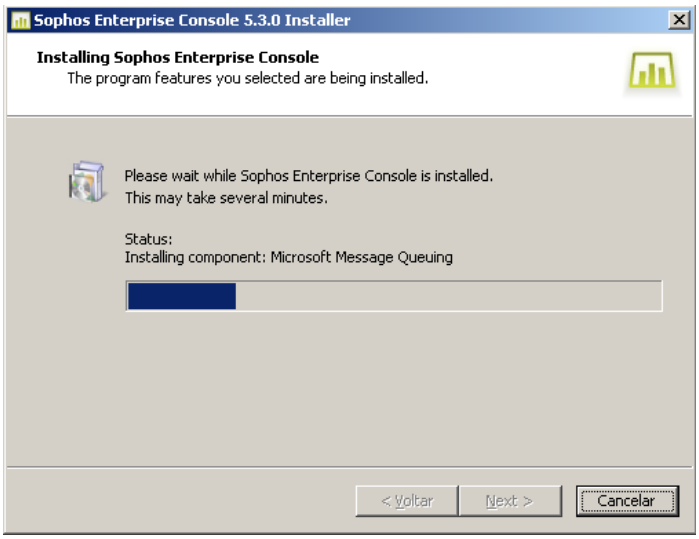
3.25. Na tela “Feedback to Sophos”, desmarque a opção “I agree” e clique em “Avançar”.



3.26. Na tela “Ready to Install”, clique no botão “Install” para iniciar a instalação.



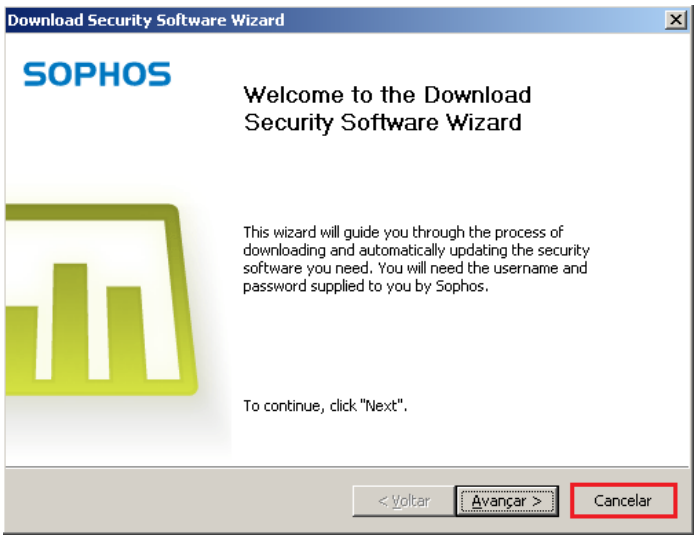
3.27. Aguarde a instalação finalizar.



3.28. Após finalizar a instalação, será solicitado um logoff, clique no botão “Concluir”, o logoff será realizado (em alguns casos pode se solicitado a reinicialização).

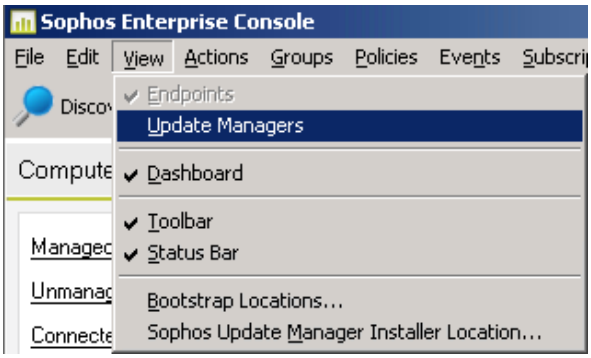
3.29. Faça login no servidor, após isto o Sophos Enterprise Console irá iniciar automaticamente.

3.30. Na tela “Download Security Software Wizard”, clique no botão “Cancelar”.

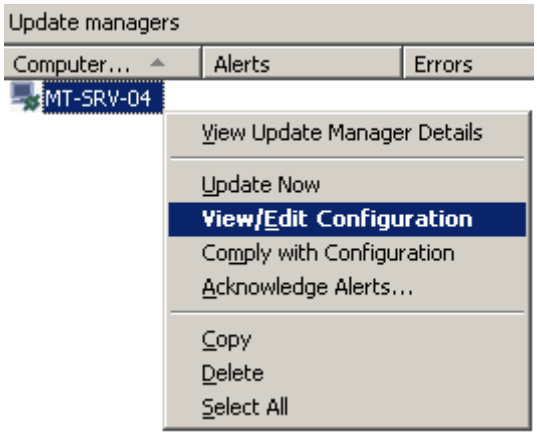


3.31. Na tela de confirmação, clique em “Sim”.

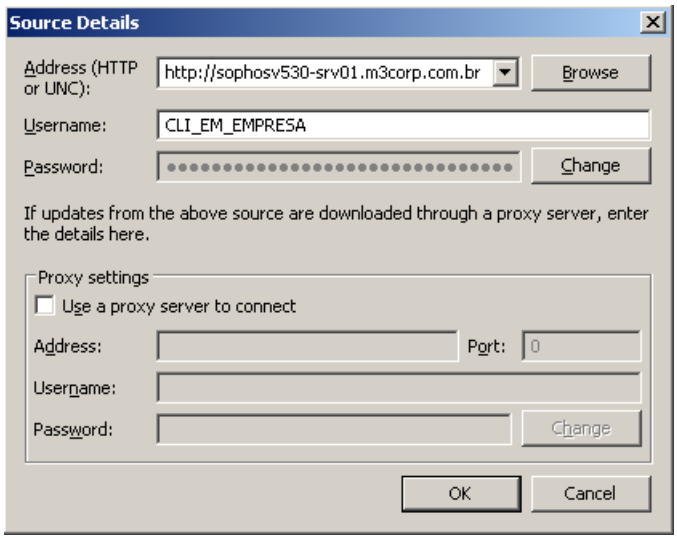
3.32. No menu bar, clique em “View” > “Update Managers (caso esta opção estiver desabilitada, pule para o próximo passo).”



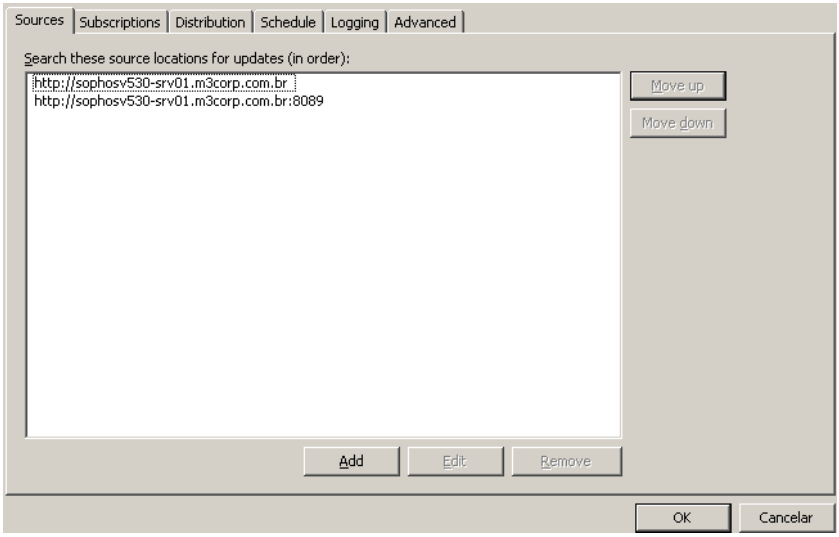
3.33. Clique com o Botão direito no servidor e clique em “View/Edit Configuration”.



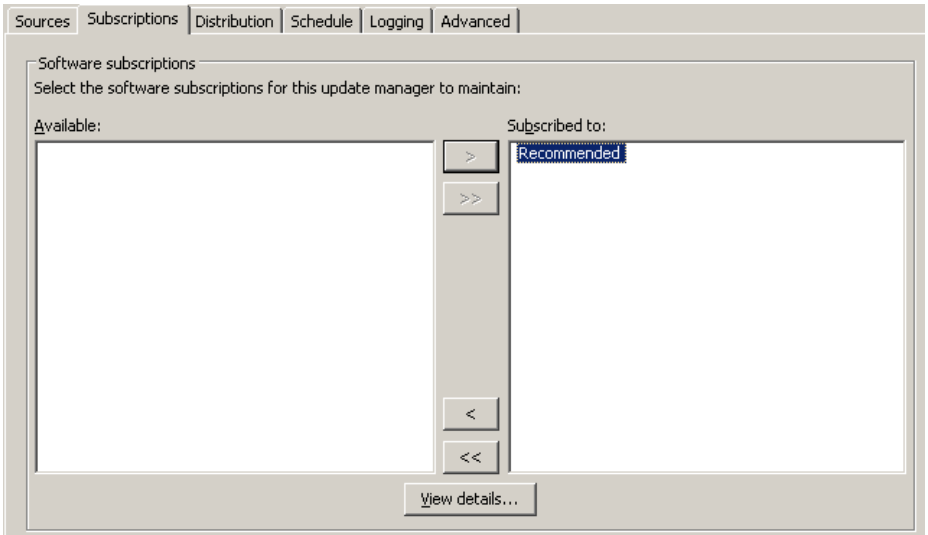
3.34. Clique no botão “Add”.
3.35. Em “Address”, informe: http://sophosv530-srv01.m3corp.com.br
3.36. Em “Username”, informe seu usuário de atualização (informado em sua licença).
3.37. Em “Password”, informe a senha do seu usuário de atualização.
3.38. Clique no botão “OK”.



3.39. Clique novamente no botão “Add”.
3.40. Em “Address”, informe: http://sophosv530-srv01.m3corp.com.br:8089
3.41. Em “Username”, informe seu usuário de atualização (informado em sua licença).
3.42. Em “Password”, informe a senha do seu usuário de atualização.
3.43. Clique no botão “OK” para salvar a nova “Source”.

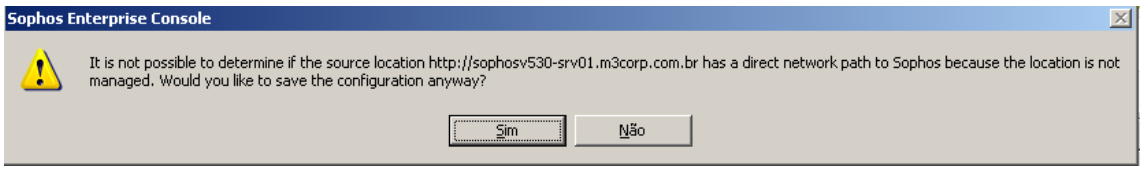


3.44. Clique na guia/aba “Subscription”, selecione o item “Recommended”, clique no botão “>” e então clique no botão “OK”.



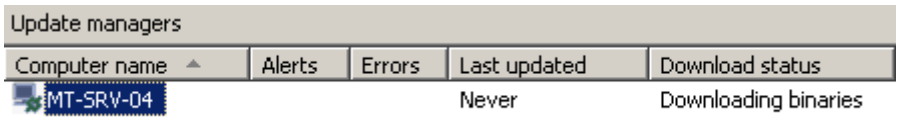
3.45. Na janela “Configure update manager”, clique no botão “OK”.

3.46. Duas mensagens serão exibidas (conforme os exemplos das imagens abaixo), clique no botão “Sim” e em seguida clique no botão “OK”:

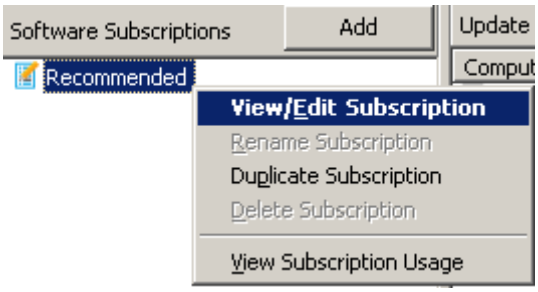


3.47. Clique com o botão direito no servidor e clique em “Update now”.

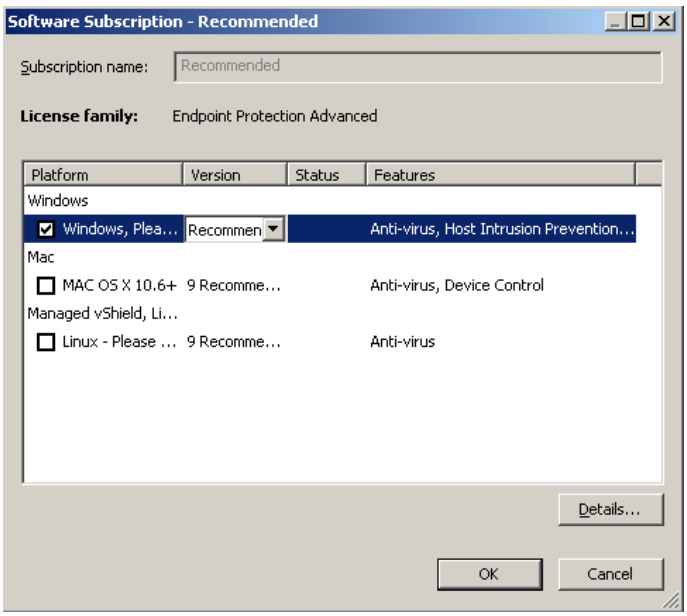
3.48. Aguarde a coluna “Download status” alterar de “Downloading binaries” para “Last checked at: <data atual>” (isto pode demorar em torno de 1 a 2 minutos).



3.49. Clique com o botão direito do mouse no “Recommended” e clique em “View/Edit Subscription”.

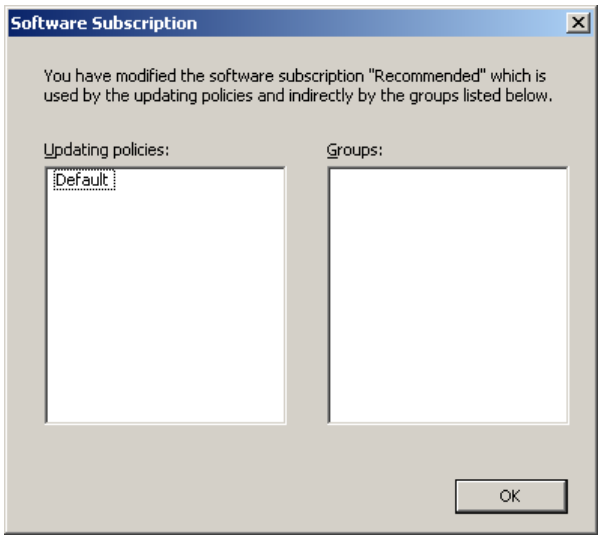


3.50. A janela “Software Subscription” irá abrir, na coluna “Platform” selecione as plataformas desejadas (onde o servidor do Sophos irá fazer o download dos arquivos de instalação para as plataformas selecionadas), clique no botão “OK”.



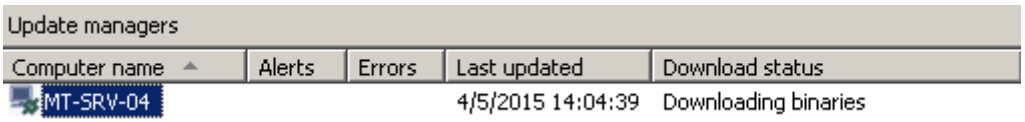
3.51. Clique no botão “OK”.

3.52. Clique no botão “OK”.

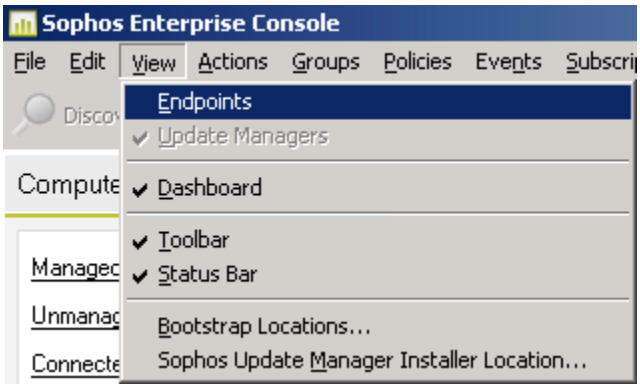


3.53. A coluna “Download status” irá voltar a indicar “Downloading binaries”, o primeiro update (onde será realizado o download dos arquivos de instalação para cada plataforma selecionada anteriormente), quando o download finalizar, a coluna “Download status” irá indicar “Last checked at: <data>”, é necessário aguardar o download finalizar para:

- Fazer a instalação do Sophos Endpoint nas estações.
- Configurar algumas políticas como “Application Control” e “Data Control”, que dependem de algumas informações que são coletadas via update.



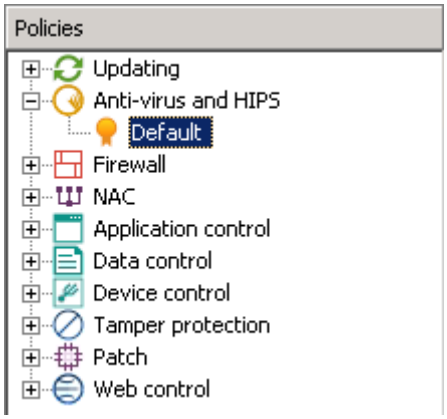
3.54. Para voltar a visualizar o painel dos “endpoints”, clique em “View” > “Endpoints”.



4. Configurações recomendadas

Neste item, será demonstrado às configurações recomendadas para novas implementações do Sophos, onde o foco é configurar o Sophos para não causar nenhum bloqueio indesejado, mantendo a proteção contra malwares. Após o período de implementação, é recomendado ativas os módulos do Sophos de forma gradual.

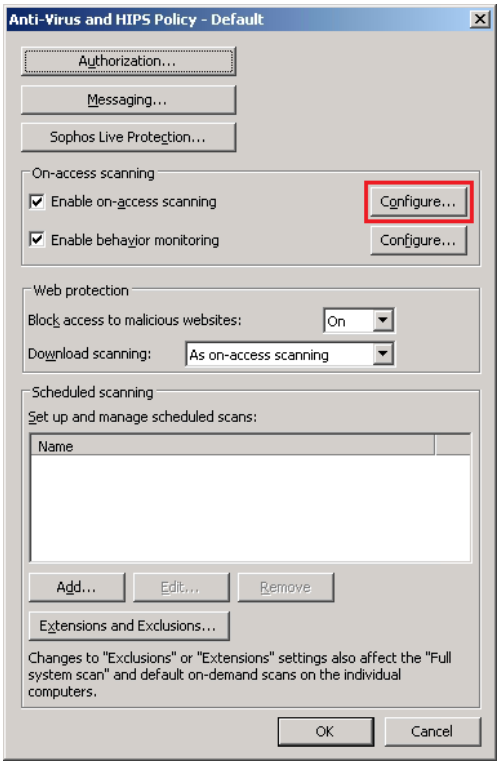
4.1. Anti-virus and HIPS



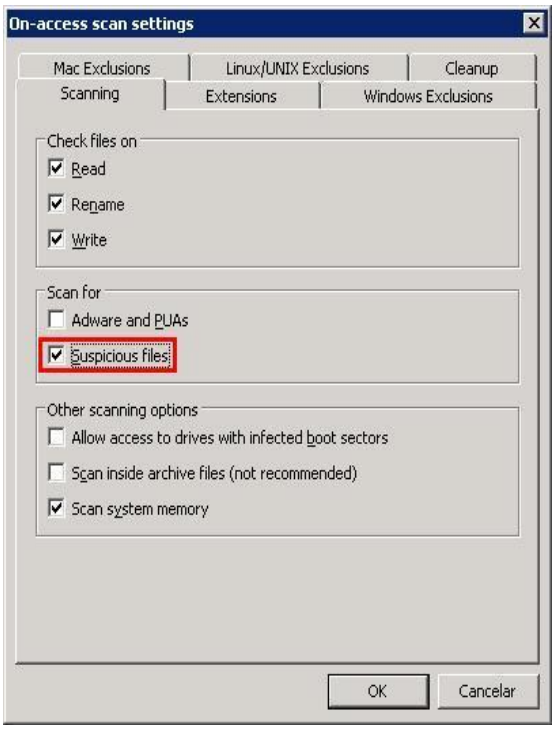
4.1.1. No Sophos Enterprise Console, expanda o item “Anti-virus and HIPS”.

4.1.2. Clique duas vezes na política de Antivírus e HIPS a ser editada (ou clique com o botão direito e clique em “View/Edit Policy”)

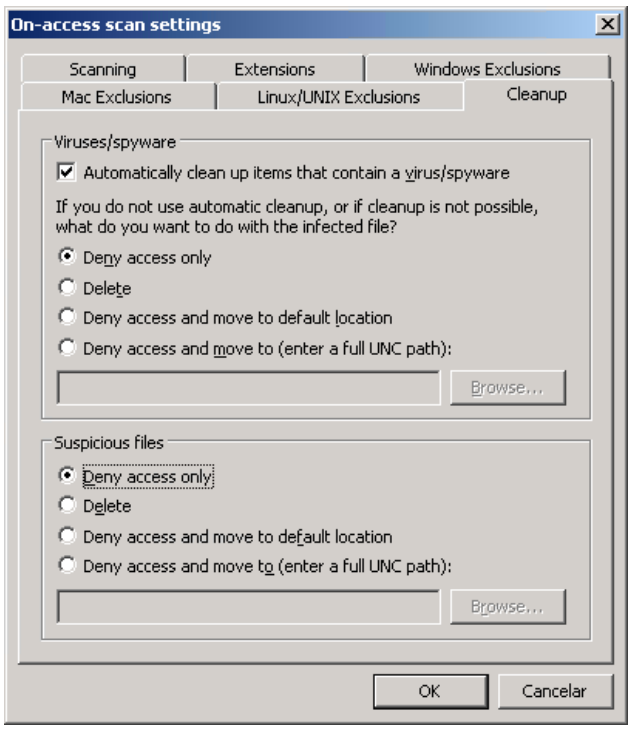
4.1.3. Em “Enable on-access scanning”, clique em “Configure...”.



4.1.4. Na guia/aba “Scanning” marque a opção “Suspicious files (HIPS)” para habilitar a analise por arquivos suspeitos.

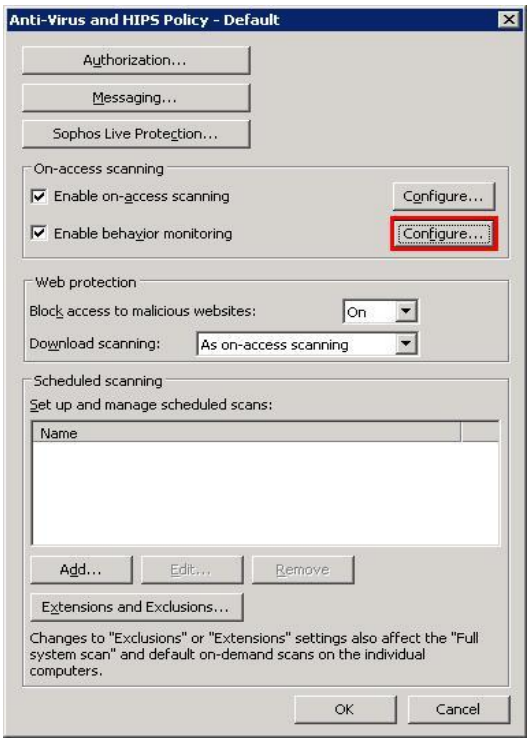


4.1.5. Na guia “Cleanup”, marque a opção “Automatically clean up item that contain a vírus/spyware”, e selecione as ações que devera ser usadas caso o cleanup não esteja disponível ou caso a opção de cleanup não esteja marcada, como o exemplo da imagem abaixo:

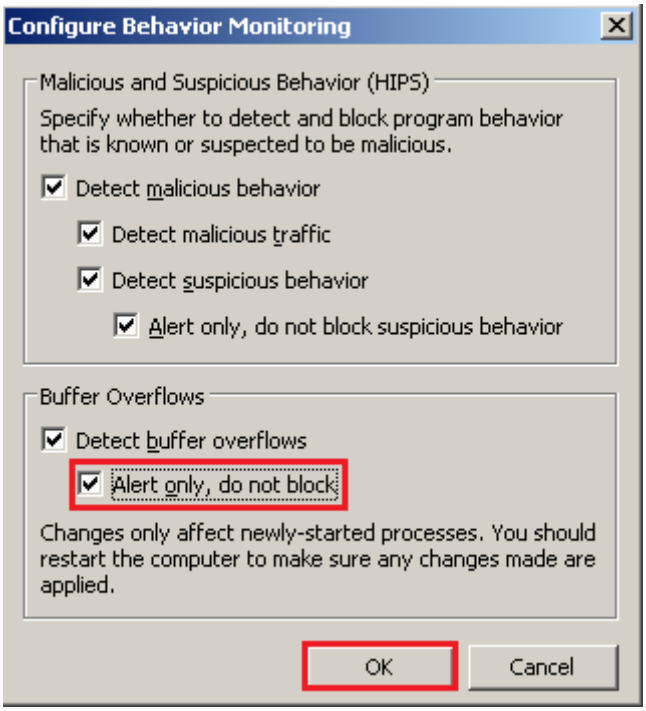


4.1.6. Clique no botão “OK”.

4.1.7. Em “Enable behavior monitoring” clique em “configure...”

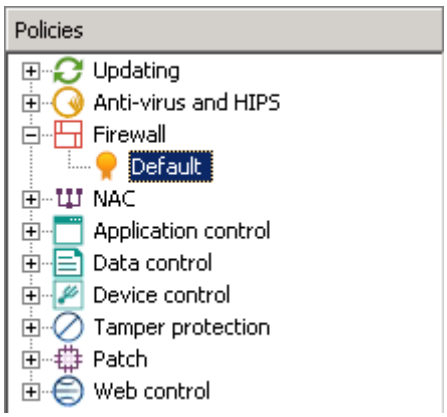


4.1.8. Em Buffer Overflows, habilite a opção “Alert only, do not block” e clique no botão “OK”.



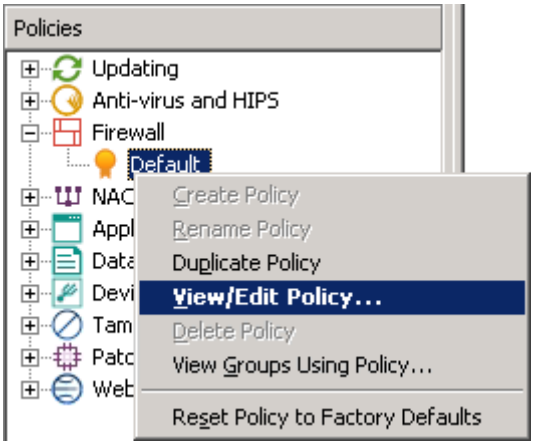
4.1.9. Aplique as alterações clicando no botão “OK”.

4.2. Firewall



4.2.1. No quadro “Policies”, expanda o item “Firewall”.

4.2.2. Clique com o botão direito na política “Default” (dentro o item “Firewall”) e clique em “View/Edit Policy”.



4.2.3. Na tela “Welcome to the firewall policy wizard”, clique em “Avançar”

4.2.4. Na tela “Configure firewall”, escolha a opção “Single location” e clique em “Avançar”

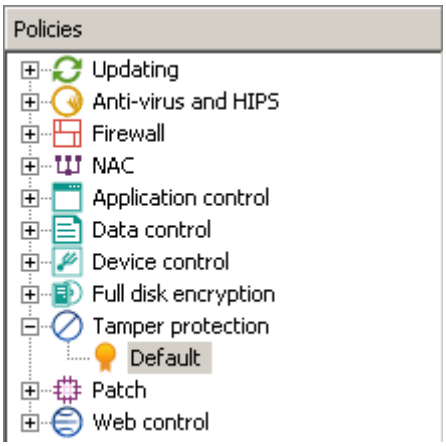
4.2.5. Na tela “Operational mode”, escolha a opção “Monitor” e clique em “Avançar”

4.2.6. Na tela “File and printer sharing”, escolha a opção “Allow file and printer sharing’ e clique em “Avançar”

4.2.7. Clique em “Concluir” para finalizar o assistente

4.3. Tamper protection

O Tamper protection impede que usuários não autorizados editem as políticas bem como desinstalar o Sophos Endpoint do computador, com isto, será necessário informar uma senha que foi previamente configurada nas políticas da console.



4.3.1. No quadro “Policies”, expanda o item “Tamper protection”.

4.3.2. Clique com o botão direito na política “Default” (dentro o item “Tamper protection”) e clique em “View/Edit Policy”.

4.3.3. Marque a opção “Enable tamper protection”.

4.3.4. Clique no botão “Set...”.

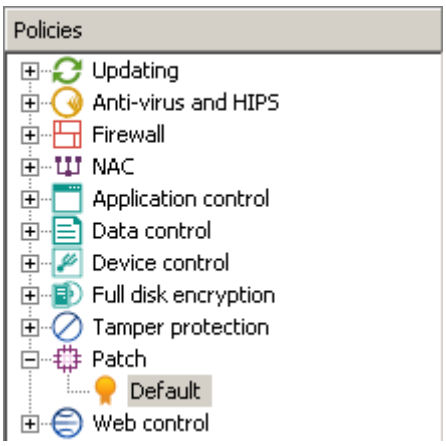
4.3.5. Em “Password”, informe a senha desejada.

4.3.6. Em “Confirm password”, confirme a senha e clique no botão “OK”.

4.3.7. Clique no botão “OK”.

4.4. Patch

Atualmente, 90% dos ataques podem ser evitados com um patch existente. No entanto, muitos computadores continuam em risco, pois identificar os computadores que estão sem um determinado patch pode ser uma tarefa difícil. Alem de identificar os computadores que estão sem algum patch de correção, o Sophos Patch Assessment qualifica os patchs e identifica as ameaças que exploram a vulnerabilidade que o patch pode corrigir.



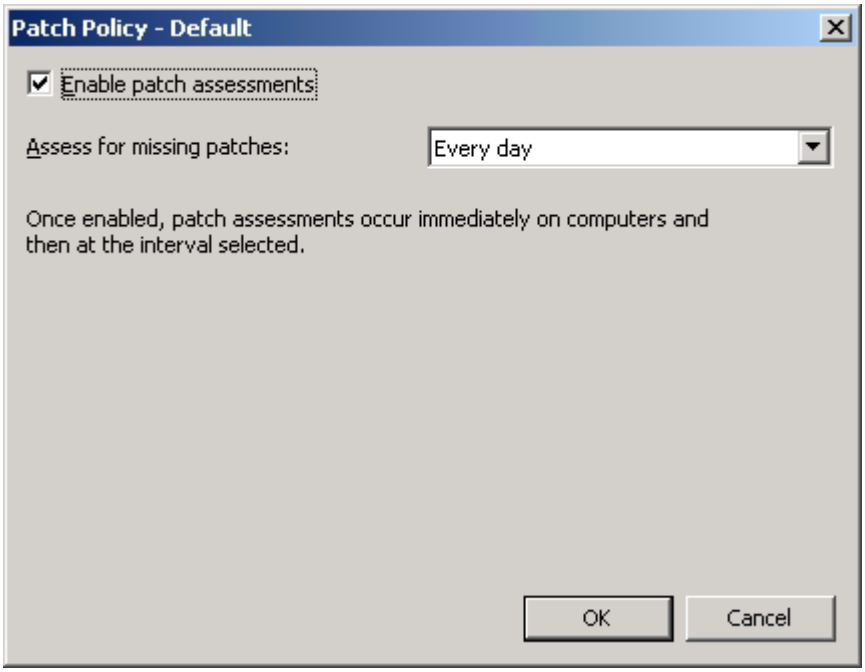
4.4.1. No quadro “Policies”, expanda o item “Path”.

4.4.2. Clique com o botão direito na política “Default” (dentro o item “Path”) e clique em “View/Edit Policy”.

4.4.3. Marque a opção “Enable patch assessments”.

4.4.4. Em “Assess for missing patchs”, selecione “Every day”.

4.4.5. Clique no botão “OK”



5. Instalando os endpoints (deploy)

Existem várias formas para realizar a instalação do software do endpoint, no entanto não é necessário realizar todas as opções. Para fazer o deploy, consulte o artigo AA-00218 em nossa base de conhecimentos, que descreve alguns métodos de deploy recomendados:

http://suporte.m3corp.com.br/article/AA-00218